

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

SHEILA POTOCHNIK,

Case No. 13-CV-2093 (PJS/JJG)

Plaintiff,

v.

ORDER

WALTER CARLSON, acting in his individual capacity as a Sergeant for the City of Minneapolis Police Department; CITY OF ANOKA; CITY OF BLOOMINGTON; CITY OF BROOKLYN CENTER; CITY OF COON RAPIDS, CITY OF MINNEAPOLIS; MICHAEL CAMPION, acting in his individual capacity as Commissioner of the Minnesota Department of Public Safety; RAMONA DOHMAN; JOHN AND JANE DOES (1-500), acting in their individual capacity as supervisors, officers, deputies, staff, investigators, employees or agents of the other law-enforcement agencies; DEPARTMENT OF PUBLIC SAFETY DOES (1-30), acting in their individual capacity as officers, supervisors, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety; ENTITY DOES (1-50), including cities, counties, municipalities, and other entities sited in Minnesota and federal departments and agencies,

Defendants.

Kenneth H. Fukuda, Jonathan A. Strauss, Lorenz F. Fett, Jr., Sonia Miller-Van Oort, and Mark H. Zitzewitz, SAPIENTIA LAW GROUP, PLLC, for plaintiff.

Peter G. Mikhail and Mary D. Tietjen, KENNEDY & GRAVEN, CHARTERED, for defendant Walter Carlson.

Oliver J. Larson, MINNESOTA ATTORNEY GENERAL'S OFFICE, for defendants Michael Campion and Ramona Dohman.

Plaintiff Sheila Potocnik brings numerous claims against numerous defendants for unlawfully disclosing or obtaining information contained in her driver's-license record. This matter is before the Court on two motions: the motion of defendants Michael Campion and Ramona Dohman (collectively, "the Commissioners") to dismiss for failure to state a claim and the motion of defendant Walter Carlson for partial judgment on the pleadings. For the reasons stated below, both motions are granted.

I. BACKGROUND

A. Allegations against Sergeant Carlson

Defendant Walter Carlson is a Minneapolis police sergeant. Compl. ¶ 12. He is also the father of a woman ("Ms. Carlson") who was in a 10-year relationship with Potocnik's brother, Duane DeMeules. Compl. ¶ 29. DeMeules and Ms. Carlson had two children together. Compl. ¶ 29. After that relationship ended, Potocnik and Ms. Carlson remained friendly. Compl. ¶ 31. Sergeant Carlson, however, disliked DeMeules and frequently threatened him with violence. Compl. ¶ 38.

In 2010, Potocnik called Ms. Carlson on her brother's behalf to ask whether he could visit his children. Compl. ¶ 32. Ms. Carlson initially agreed to limited visitation. Compl. ¶ 33. Potocnik called back a couple of times to set up a visitation schedule, but initially received no response. Compl. ¶ 35. Eventually, Ms. Carlson called Potocnik to say that she had changed her mind and that she preferred to have a formal visitation schedule set up by a court or a mediator. Compl. ¶ 36. Potocnik said that she understood and would inform her brother. Compl. ¶ 37.

On October 8, 2010, Sergeant Carlson called Potocnik's cell phone from the Minneapolis Police Department. Compl. ¶ 39. Carlson yelled and swore at Potocnik, telling her not to "call

his f***cking daughter again” and saying that he “didn’t want Potocnik’s f***ing brother or anybody in their family around his grandkids.” Compl. ¶ 41.

During the phone call, Carlson revealed to Potocnik that he knew that she lived in St. Michael, that she worked at North Memorial Hospital, and that she was in school for law enforcement. Compl. ¶¶ 43-45. Carlson also said that he knew that Potocnik was planning to take the Minnesota Board of Peace Officers Standards and Training Test, and Carlson demanded to know when she would take it. If she refused to tell him, Carlson said, “I can easily find out from other sources.” Compl. ¶ 47. Carlson also referred to Potocnik’s then-boyfriend, who was a former Minneapolis police officer, and Carlson derogatorily referred to Potocnik’s sister Laura, who had been murdered in Carlson’s precinct in 2005. Compl. ¶ 48-56. Carlson said that he “knew [Laura] very well” and that he “kn[ew] what happened. Real great family.” Compl. ¶¶ 55-56.

Potocnik ended the phone call, which left her frightened for her safety. Compl. ¶¶ 44, 57. Over the next hour and a half, Carlson tried calling back several times. Compl. ¶ 58. Potocnik eventually called Carlson, who began screaming and verbally attacking Potocnik, her brother, and her father. Compl. ¶¶ 59-65. He also brought up Potocnik’s sister Laura again. Compl. ¶ 71. Potocnik asked Carlson how he was getting all of this information. Compl. ¶ 66. Carlson admitted to using his computer at the Minneapolis Police Department to find information about Potocnik and her family. Compl. ¶ 67.

Potocnik complained to the Minneapolis Police Department's Internal Affairs unit. Compl. ¶ 72. Scott Zierden was assigned by the department to conduct an investigation.¹ Compl. ¶ 73. Zierden told Potocnik that Carlson admitted accessing the Department of Vehicle Services ("DVS") database to obtain information about Potocnik and her family. Compl. ¶ 85. The case was referred to the St. Paul City Attorney for a criminal investigation. Compl. ¶ 86. During the investigation, the Department of Public Safety conducted an audit of Carlson's use of the DVS database. Compl. ¶ 88. The audit revealed that, since 2003, Carlson had repeatedly accessed records unrelated to official business or work-related assignments. Compl. ¶ 88. Beginning in 2004, Carlson had accessed Potocnik's DVS record 26 times, including twice on the day that he made the threatening calls to her. Compl. ¶¶ 112-13. Carlson also accessed her DVS record after the threatening phone calls, and continued to access her record during the internal-affairs investigation. Compl. ¶¶ 114-15.

Potocnik later requested an audit of her DVS record. Compl. ¶ 152-53. The audit disclosed that Potocnik's DVS record has been accessed over 75 times since 2004 by various officers from various cities and various public agencies. Compl. ¶ 3; *see also* Compl. ¶¶ 101-07. The audit indicated that the inquiring officers had used Potocnik's name, not her license-plate number, to access her record. Compl. ¶ 164.

¹Potocnik alleges that Zierden should have recused himself from the investigation, because he admitted that he was a friend of Carlson's. Compl. ¶¶ 77-78. Potocnik also alleges that the investigation was botched and that, as a result, criminal charges against Carlson were dismissed and Carlson was allowed to return to work without being punished. Compl. ¶¶ 86-98. Potocnik does not base any claims on these allegations, however.

B. Allegations against the Commissioners

Defendant Michael Campion was formerly the Commissioner of the Department of Public Safety (“DPS”), which created and maintains the DVS database. Compl. ¶¶ 24, 99. During Campion’s tenure, the DVS database was developed into its current format. Compl. ¶ 196. Defendant Ramona Dohman is Campion’s successor. Compl. ¶ 25. Both Campion and Dohman have been involved in law enforcement for many years. Compl. ¶¶ 190-95.

Potocnik alleges that the Commissioners are well aware of widespread misuse of the DVS database, but they have ignored the problem and failed to safeguard the database, provide adequate training, or correct abuses. Compl. ¶¶ 197, 200. And even if the Commissioners did not actually know of the misuse of the DVS database, Potocnik alleges, they were nevertheless reckless or grossly negligent in supervising their subordinates who operated the database.² Compl. ¶¶ 150-51.

II. ANALYSIS

Potocnik brings (1) claims under the Driver’s Privacy Protection Act (“DPPA”), 18 U.S.C. §§ 2721 et seq., (2) constitutional and statutory claims under 42 U.S.C. § 1983, and (3) a state-law claim of invasion of privacy. The Commissioners move to dismiss all of the claims against them. Sergeant Carlson moves for judgment on the pleadings as to the § 1983 and

²In addition to bringing claims against the Commissioners, Potocnik also asserts claims against various unnamed employees, agents, and independent contractors of DPS. Compl. ¶ 28. The Commissioners argue that the claims against these unnamed DPS defendants should be dismissed for the same reasons that the Court should dismiss the claims against the Commissioners. The Court agrees that Potocnik’s claims against the unnamed DPS defendants rest on the same factual and legal bases as her claims against the Commissioners and that the two sets of claims should rise or fall together. Accordingly, any reference by the Court to the Commissioners is intended to include the unnamed DPS defendants.

invasion-of-privacy claims and argues that, insofar as the DPPA claims are based on acts that occurred before August 1, 2009, those claims are barred by the statute of limitations.

A. Standard of Review

In reviewing a motion to dismiss for failure to state a claim under Fed. R. Civ. P. 12(b)(6), the court must accept as true all of the factual allegations in the complaint and draw all reasonable inferences in the plaintiff's favor. *Aten v. Scottsdale Ins. Co.*, 511 F.3d 818, 820 (8th Cir. 2008). Although the factual allegations in the complaint need not be detailed, they must be sufficient to "raise a right to relief above the speculative level" *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). The complaint must "state a claim to relief that is plausible on its face." *Id.* at 570. In assessing the sufficiency of the complaint, the court may disregard legal conclusions that are couched as factual allegations. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009).

Ordinarily, if the parties present, and the court considers, matters outside of the pleadings, a motion to dismiss must be treated as a motion for summary judgment. Fed. R. Civ. P. 12(d). But the court may consider materials that are necessarily embraced by the complaint, as well as exhibits attached to the complaint, without converting the motion into one for summary judgment. *Mattes v. ABC Plastics, Inc.*, 323 F.3d 695, 697 n.4 (8th Cir. 2003).

A motion for judgment on the pleadings under Fed. R. Civ. P. 12(c) is assessed under the same standards as a motion to dismiss under Fed. R. Civ. P. 12(b)(6). *Ashley Cnty. v. Pfizer, Inc.*, 552 F.3d 659, 665 (8th Cir. 2009).

B. The DPPA

1. The Commissioners

Potocnik alleges that, by creating and maintaining the DVS database without adequate safeguards despite being aware that it is frequently misused, the Commissioners knowingly disclosed her personal information in violation of the DPPA. Compl. ¶¶ 128-30. Potocnik's DPPA claim against the Commissioners fails, however, because she has not plausibly alleged that the Commissioners had an impermissible purpose when they disclosed her personal information.

The DPPA prohibits a state department of motor vehicles and its officers, employees, and contractors from “knowingly disclos[ing] or otherwise mak[ing] available to any person or entity” either “personal information” or “highly restricted personal information” obtained by the department in connection with a motor-vehicle record.³ 18 U.S.C. § 2721(a). (In this order, the Court will collectively refer to “personal information” and “highly restricted personal information” as “personal information.”) The DPPA carves out various exceptions to this prohibition; for example, the DPPA authorizes disclosure of personal information “[f]or use by any government agency, including any court or law enforcement agency, in carrying out its functions” 18 U.S.C. § 2721(b).

³ “[P]ersonal information” is defined as “information that identifies an individual, including an individual’s photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver’s status.” 18 U.S.C. § 2725(3). “[H]ighly restricted personal information” is defined as “an individual’s photograph or image, social security number, [and] medical or disability information” 18 U.S.C. § 2725(4).

The DPPA provides for both civil and criminal enforcement. A person who knowingly violates the DPPA is subject to a criminal fine. 18 U.S.C. § 2723(a). The Attorney General may impose civil penalties on any state department of motor vehicles that has “a policy or practice of substantial noncompliance” with the DPPA. 18 U.S.C. § 2723(b). And the subject of a motor-vehicle record may sue any “person who knowingly obtains, discloses or uses [his] personal information, from a motor vehicle record, for a purpose not permitted under this chapter” 18 U.S.C. § 2724.

A close reading of § 2721 (which prohibits certain disclosures) and § 2724 (which creates a cause of action for prohibited disclosures) reveals that they differ in a subtle but important way. Section 2721(a) prohibits all disclosure of personal information except for the purposes identified in § 2721(b). Thus § 2721 implies that disclosure is prohibited unless the *person making the disclosure* can prove that he or she had a *good* purpose. Section 2724, however, provides a cause of action against a person who knowingly obtains, discloses, or uses personal information “for a purpose not permitted under this chapter” Thus § 2724 requires the *plaintiff* to plead and prove that the defendant had a *bad* purpose. *See Thomas v. George, Hartz, Lundeen, Fulmer, Johnstone, King, & Stevens, P.A.*, 525 F.3d 1107, 1110-14 (11th Cir. 2008) (plaintiff bears the burden of proof to show an impermissible purpose under § 2724); *Smythe v. City of Onamia*, No. 12-3149 (ADM/LIB), 2013 WL 2443849, at *4 (D. Minn. June 5, 2013) (“The few courts to have ruled on the issue have held the plaintiff has the burden of proving each element of the civil claim, including whether the retrieval was for a ‘purpose not permitted’ by the Act.”).

To properly plead a DPPA claim, then, Potocnik must plausibly allege not only that a defendant knowingly obtained, disclosed, or used her personal information, but that the defendant did so for a purpose not permitted under the DPPA. Potocnik argues, however, that a person who discloses personal information to a recipient who has an impermissible purpose for obtaining the information can be held liable, even if the person making the disclosure has a permissible purpose for disclosing the information.⁴ The Court disagrees. When a statute makes a “person” liable for taking action “for a purpose,” the statute is referring to the purpose of the person taking the action. Of course, when the person who makes a disclosure is *aware* of the intended use of the information by the person to whom the disclosure is made, the purpose of the person disclosing the information will generally be the same as the purpose of the person obtaining the information. If that purpose is not permitted by the DPPA, then both the person who discloses the information and the person who obtains the information could be held liable under § 2724(a). But the fact that the two purposes will often coincide does not mean that they will *always* coincide. If the disclosure was made for a permissible purpose, then the person making the disclosure cannot be held liable under the DPPA, irrespective of the purpose of the person who sought the information. *See Nelson v. Jesson*, No. 13-340 (RHK/JJK), 2013 WL 5888235, at *3 (D. Minn. Nov. 1, 2013) (“It is not enough that [the Commissioners] disclosed information to Schlener and *he* acted with an impermissible purpose, the Commissioners *themselves* must have acted with such a purpose. This is the only possible interpretation, given

⁴Potocnik does not expressly make this argument; instead, she contends that the word “knowingly” in § 2724 does not apply to the “purpose” element. This argument only makes sense if the relevant “purpose” could be that of someone *other* than the person making the disclosure; it is hard to imagine how anyone who “knowingly obtains, discloses or uses” information for a “purpose” would not know his or her *own* purpose.

the plain language of the statute.”); *Kiminski v. Hunt*, No. 13-185 (JNE/TNL), 2013 WL 6872425, at *6 (D. Minn. Sept. 20, 2013) (“Under the plain language of the statute, the person who obtains, discloses, or uses the information must do so *for* an impermissible purpose.”).

To plead a valid DPPA claim against the Commissioners, then, Potocnik must plausibly allege not only that the Commissioners knowingly disclosed her information, but also that the Commissioners had an impermissible purpose in doing so. Potocnik does not contend that the Commissioners knew her, knew that anyone had sought her personal information, or disclosed her personal information for a impermissible purpose. Instead, Potocnik argues that the “purpose” that matters is the Commissioners’ purpose for creating and maintaining the entire DVS database — which purpose, Potocnik alleges, was to facilitate the widespread misuse of DVS records. In other words, Potocnik alleges that the purpose of the Commissioners in creating and maintaining the DVS database of the State of Minnesota was not to assist public employees and others in carrying out their legitimate functions, but rather to help rogue officials like Carlson obtain driver’s-license information for nefarious purposes. The basis for this rather remarkable allegation is that, according to Potocnik, the Commissioners were aware of widespread misuse of the DVS database but failed to do anything to prevent or stop it.

This is, to put it mildly, an implausible allegation. The fact that the Commissioners were aware of widespread misuse of the DVS database does not mean that their purpose in creating and maintaining the database was to facilitate that misuse. Presumably those who maintain the Internet know that it is widely misused to transmit child pornography. And presumably those who maintain the nation’s highways know that they are widely misused to transport illegal drugs. Alleging that the Commissioners maintain the DVS database for the *purpose* of facilitating

misuse of the database is as absurd as alleging that those who maintain the Internet do so for the *purpose* of facilitating the transmission of child pornography or that those who maintain the nation's highways do so for the *purpose* of facilitating the transportation of illegal drugs.

The DPPA permits the Commissioners to disclose personal information for numerous reasons, including “[f]or use by any government agency, including any court or law enforcement agency, in carrying out its functions . . .” 18 U.S.C. § 2721(b)(1). As other courts have noted, there are a “broad range of permissible uses that a governmental agency might have for motor vehicle data.” *Kost v. Hunt*, No. 13-583 (JNE/TNL), 2013 WL 6048921, at *12 (D. Minn. Nov. 15, 2013). And the number of permissible uses of the DVS database undoubtedly dwarf the number of impermissible uses — just as the number of permissible uses of the Internet or of the nation's highways dwarf the number of impermissible uses.

Every one of the individuals alleged to have impermissibly accessed Potocnik's information is a law-enforcement officer who has a legitimate reason to have frequent and ready access to the DVS database. Compl. ¶¶ 102-07. In addition, as Potocnik herself alleges, the database is password-protected so that *only* those who have a legitimate reason to use it are given access. Compl. ¶¶ 180. Under these circumstances, it is not remotely plausible to suggest that the purpose of the Commissioners in creating and maintaining the entire DVS database for the State of Minnesota was to facilitate unlawful uses of driver's-license information. *Cf. Iqbal*, 556 U.S. at 679 (“Determining whether a complaint states a plausible claim for relief will, as the Court of Appeals observed, be a context-specific task that requires the reviewing court to draw on its judicial experience and common sense.”).

In addition, the consequences of accepting Potocnik's argument would be staggering. According to Potocnik, the very existence of Minnesota's DVS database is illegal, because the Commissioners' purpose in establishing and maintaining that database is to facilitate its misuse. That unlawful purpose would be the same for every individual disclosure; in other words, the Commissioners' "purpose" with respect to the Potocnik disclosures was identical to their "purpose" with respect to the millions of other disclosures of DVS information. Thus, according to Potocnik, the Commissioners can be held liable every time personal information in the DVS database is disclosed, because even if the person seeking the information has a permissible purpose, the persons disclosing the information — the Commissioners — are acting with an impermissible purpose. If Potocnik's theory were accepted, the potential liability of the Commissioners would reach into the billions of dollars.

Potocnik makes an alternative argument. Even if the Commissioners did not have an evil purpose in creating and maintaining the DVS database, Potocnik argues, they nevertheless can be held liable because they acted negligently in failing to use reasonable care to prevent misuse of the database. This is at least a respectable argument, and its premise may be true — that is, it may be true that the Commissioners have not used reasonable care to prevent misuse of the DVS database. The problem for Potocnik, though, is that the DPPA does not impose a duty of care on the Commissioners. Congress generally does not tell states how they must manage the regulatory information that they collect for their own purposes. If Congress intended to make an exception for driver's-license data, one would expect Congress to have been very clear that it was imposing a duty of care on the motor-vehicle departments of 50 states, and one would expect that the Department of Transportation would have been directed to promulgate regulations to give the

states guidance about how they were expected to maintain their driver's-license databases. *See Will v. Mich. Dep't of State Police*, 491 U.S. 58, 65 (1989) (“Congress should make its intention ‘clear and manifest’ if it intends to pre-empt the historic powers of the States” (citation omitted)).

But nothing in the DPPA explicitly or implicitly imposes a privately enforceable duty to use reasonable care on the states. To the contrary, the statute rather strongly implies that Congress did *not* intend to impose such a duty. The DPPA authorizes the subject of a motor-vehicle record to sue a “person” who unlawfully obtains, discloses, or uses that record, but the DPPA specifically *excludes* states and state agencies from the definition of “person[s]” who may be sued. *See* 18 U.S.C. § 2725(2). Instead, the DPPA leaves enforcement against state agencies to the Attorney General, who is empowered to impose civil penalties against state motor-vehicle departments — not for failing to use reasonable care, but for having a “policy or practice of substantial noncompliance” with the DPPA. 18 U.S.C. § 2723(b). Taken together, these provisions quite clearly indicate that Congress did *not* intend to impose a duty of reasonable care on state agencies that would be enforceable in private litigation.⁵

⁵Under 42 U.S.C. § 1983, as under the DPPA, a state is not “person” who can be sued. *Will v. Mich. Dep't of State Police*, 491 U.S. 58, 64 (1989). Nevertheless, under the *Ex parte Young* doctrine, § 1983 permits actions for injunctive relief against state officials acting in their official capacities. *Kentucky v. Graham*, 473 U.S. 159, 167 n.14 (1985); *Will*, 491 U.S. at 71 n.10. One could argue, therefore, that the DPPA likewise permits suits for *injunctive* relief against state officials acting in their official capacities. Because the DPPA specifically provides for a separate civil-penalty provision against state motor-vehicle departments, however, the Court interprets the DPPA to preclude even suits for prospective relief against state officials acting in their official capacities. *See Seminole Tribe of Fla. v. Florida*, 517 U.S. 44, 74 (1996) (“where Congress has prescribed a detailed remedial scheme for the enforcement against a State of a statutorily created right, a court should hesitate before casting aside those limitations and permitting an action against a state officer based upon *Ex parte Young*”).

Potocnik relies on *Gordon v. Softech International, Inc.*, in which a divided panel of the Second Circuit held that the DPPA imposes a duty of care on resellers of motor-vehicle records to ensure that the records are not being misused. 726 F.3d 42, 53 (2d Cir. 2013) (2-1 decision). The majority found such a duty in the “language of the statute, its structure, and its legislative history” *Id.* In particular, the majority reasoned that if a reseller of motor-vehicle records can resell those records for only a permitted purpose, then the reseller logically must make some inquiry into the purpose of the buyer before the reseller can conclude that disclosure is permitted. *Id.* at 53-54.

With respect to the *Gordon* majority, the Court doubts the DPPA imposes a duty to use reasonable care on private resellers of motor-vehicle records. But even if *Gordon* was correctly decided, it does not help Potocnik in this case. *Gordon* reasoned that, when a reseller puts information up for sale, the reseller cannot be doing so for a lawful purpose unless the reseller makes some inquiry into the purpose of the buyer. Here, however, Potocnik is not suing a reseller, but instead the Commissioners who created and maintain the DVS database. The Commissioners did not sell information on the open market (or, if they did, that is not the basis of Potocnik’s claim). Instead, the Commissioners created a password-protected database for a specific population of law-enforcement officers and other users who have many and frequent legitimate uses for the information. *Gordon* therefore does not persuade the Court that state governments owe a federally imposed duty of care in creating and maintaining driver’s-license databases. (The Second Circuit may not disagree; it quite explicitly limited its holding to private resellers. *Gordon*, 726 F.3d at 57 n.14.)

Finally, even if the Commissioners could violate the DPPA by negligently setting up and maintaining the DVS database, they would be protected by qualified immunity because it surely is not clearly established that they owe a duty of care. *See Williams v. Jackson*, 600 F.3d 1007, 1012 (8th Cir. 2010) (government officials performing discretionary functions are protected from civil damages by qualified immunity insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known); *cf. Roth v. Guzman*, 650 F.3d 603, 612 (6th Cir. 2011) (government officials were entitled to qualified immunity on DPPA claim because it was not clearly established that they could be liable for a recipient's impermissible use). The Court therefore grants the Commissioners' motion and dismisses Potocnik's DPPA claims against them.

2. Sergeant Carlson

Carlson does not dispute that Potocnik has pleaded a plausible DPPA claim against him. He argues, however, that the statute of limitations bars Potocnik from recovering for any acts that occurred prior to August 1, 2009 — four years prior to the date that Potocnik filed this lawsuit. ECF No. 1.

The parties agree that DPPA claims are subject to the statute of limitations in 28 U.S.C. § 1658(a), which provides that a claim within its purview “may not be commenced later than 4 years after the cause of action accrues.” What the parties dispute is when a DPPA claim “accrues” for purposes of the statute. Potocnik argues that the Court should apply the discovery rule, under which “a cause of action accrues and the statute of limitations begins to run when the plaintiff discovers, or with due diligence should have discovered, the injury which is the basis of the litigation.” *Comcast of Ill. X v. Multi-Vision Elecs., Inc.*, 491 F.3d 938, 944 (8th Cir. 2007).

Thus, Potocnik argues that the statute of limitations did not begin to run on her DPPA claim until she *learned* that Carlson had unlawfully obtained her personal information from the DVS database. Carlson argues that the Court should apply the occurrence rule, under which the cause of action accrues and the statute of limitations begins to run when the unlawful act occurs. *See Gabelli v. Sec. & Exch. Comm'n*, 133 S. Ct. 1216, 1220 (2013) (describing the “standard rule . . . that a claim accrues when the plaintiff has a complete and present cause of action” (citation and quotations omitted)). Thus, Carlson argues that the statute of limitations began to run on Potocnik’s DPPA claim when he unlawfully *obtained* her personal information from the DVS database.

Whether the discovery rule or the occurrence rule applies to DPPA claims is a difficult question. There is surprisingly little case law about whether § 1658(a)’s limitations period is triggered by the unlawful event or instead by the plaintiff’s discovery that she was injured by the unlawful event. The Eighth Circuit has said that, absent a contrary indication from Congress, the discovery rule applies in every federal-question case. *See Comcast*, 491 F.3d at 944. But the Court agrees with other judges of this District that the Supreme Court’s recent decision in *Gabelli* — which made clear that the occurrence rule is “standard” and the discovery rule is an “exception” — substantially undermines the Eighth Circuit’s statement in *Comcast*. *Gabelli*, 133 S. Ct. at 1220-21; *see Kost v. Hunt*, No. 13-583 (JNE/TNL), 2013 WL 6048921, at *6 (D. Minn. Nov. 15, 2013) (“*Gabelli* should be read as seriously undermining, if not rendering obsolete, earlier statements by the lower courts that the discovery rule operates as a default.”).

The Court acknowledges that the Eighth Circuit recently said that “*Comcast* remains good law.” *Maverick Transp., LLC v. U.S. Dep’t of Labor, Admin. Review Bd.*, 739 F.3d 1149,

1154 (8th Cir. 2014) (2-1 decision). But *Maverick Transportation* did not even mention *Gabelli*, much less attempt to reconcile *Gabelli*'s holding that the discovery rule is the "exception" with *Comcast*'s holding that the discovery rule is the norm. In any event, even if this Court were to treat the discovery rule as the norm rather than the exception, the Court would ultimately agree with Carlson that the occurrence rule should apply under the circumstances of this case.

Comcast and *Maverick Transportation* did not say that the discovery rule always applies, but only that it will be presumed to apply "absent some contrary directive from Congress" *Maverick Transp.*, 739 F.3d at 1154. And *Maverick Transportation* acknowledged that such a "contrary directive" may be implied rather than express. *Id.* The question, then, is whether Congress has implicitly directed that the occurrence rule should apply to DPPA claims.

The Court agrees with other courts that, to answer this question, it is necessary to look at the language and history of § 1658(a), as well as at the type of claim in question (in this case, a claim under the DPPA). *See Gross v. Max*, 906 F. Supp. 2d 802, 811 (N.D. Ind. 2012). Because § 1658(a) is a catch-all provision that governs widely disparate types of federal claims, it is entirely possible that the discovery rule may apply to some causes of action governed by § 1658(a) but not to others. There is nothing startling about such a result; indeed, some federal statutes that have their own specific limitations provisions incorporate the discovery rule in some cases and the occurrence rule in others depending on the nature of the underlying claim. *See Sell v. U.S. Dep't of Justice*, 585 F.3d 407, 409 (8th Cir. 2009) ("Generally, a cause of action accrues under the FTCA when a plaintiff is injured. In medical malpractice cases, however, the cause of action accrues when the plaintiff discovers the nature and cause of his injury." (citation omitted)).

Turning first to the language and history of § 1658(a): The Court is persuaded by the reasoning in *Gross v. Max*, 906 F. Supp. 2d 802 (N.D. Ind. 2012), that neither § 1658(a)'s language nor its legislative history call for the application of the discovery rule. *Id.* at 811-13. As *Gross* explained, numerous courts have found that Congress's use of the term "accrues" in a federal statute — the term used in § 1658(a) — is strong evidence that Congress intended that the occurrence rule, and not the discovery rule, apply. *Id.* at 812. In addition, as *Gross* also noted, Congress amended § 1658 in 2002 to add a subsection (b) that explicitly provides that the discovery rule should apply to certain securities claims, yet Congress left subsection (a) untouched. *Id.* at 812-13. "The fact that Congress did not originally include language like this in Section 1658(a), combined with the fact that it left subsection (a) completely unchanged when it added subsection (b), indicates that it had no intention of incorporating the discovery rule into Section 1658(a)." *Id.* The Court finds this reasoning compelling.

Gross's interpretation of "accrues" is confirmed by *Gabelli*. In *Gabelli*, the Supreme Court analyzed 28 U.S.C. § 2462, under which the limitations period begins to run when the claim "accrue[s]" (as is true under § 1658(a)). *Gabelli*, 133 S. Ct. at 1219. The Supreme Court explained that the "most natural reading" of a statute providing that the limitations period begins to run when a cause of action "accrues" is that it incorporates the occurrence rule. *Id.* at 1220-21. As the Supreme Court stated, "[i]n common parlance a right accrues when it comes into existence" *Id.* at 1220 (citation and quotations omitted).

Potocnik tries to distinguish *Gabelli* on the ground that, in *Gabelli*, the Court held that the Securities and Exchange Commission ("SEC") is not entitled to the benefit of the discovery rule when it is bringing an enforcement action for civil penalties. *Id.* at 1224. Potocnik points out

that the Court explained that the SEC is not like an ordinary civil plaintiff who has no reason to suspect fraud; one of the SEC's core missions is to investigate and uncover fraud, and it has broad powers to subpoena documents and witnesses even before filing suit. *Id.* at 1221-22.

According to Potocnik, this distinguishes *Gabelli* from her case, as she is a private party.

But Potocnik ignores the fact that the Supreme Court made this statement only *after* first holding that use of the word “accrue[s]” in a statute creates a presumption that the occurrence rule should apply. The Court then acknowledged that, notwithstanding § 2462’s use of the word “accrue[s],” the discovery rule ordinarily applies to fraud claims. *Id.* at 1221. But the Court went on to hold that, even in fraud cases, the SEC is not entitled to the benefit of the discovery rule. *Id.* at 1222-24. The language on which Potocnik relies is a part of the Court’s justification for this latter holding.

Because Potocnik is not bringing a fraud claim, *Gabelli*’s discussion of how the SEC differs from private plaintiffs is irrelevant. What matters for purposes of this case is that the Supreme Court began its analysis in *Gabelli* by holding that the word “accrue,” in the *absence* of fraud, normally calls for the application of the occurrence rule. As § 1658(a) uses the word “accrue,” and as Potocnik is not bringing a fraud claim, *Gabelli* dictates that the “most natural reading” of § 1658(a) is that it incorporates the occurrence rule.

The next step, then, is to determine whether anything about a DPPA claim would justify application of the discovery rule, notwithstanding the presumption established by *Gabelli* that a statutory limitations period that begins when a cause of action “accrues” is triggered by occurrence, not discovery. This is a close question. Potocnik’s argument that the discovery rule should apply because the average person has no reason to know when her rights under the DPPA

have been violated has some force. But the Court is nevertheless persuaded that the occurrence rule should apply, for two reasons.

First, the Supreme Court decided, in a strikingly similar factual context, that the occurrence rule — and not the discovery rule — should apply to claims brought under the Fair Credit Reporting Act (“FCRA”). *See TRW Inc. v. Andrews*, 534 U.S. 19, 23 (2001). In *TRW*, the plaintiff sued after discovering that a credit-reporting agency had improperly disclosed her credit history to third parties. *Id.* at 24-25. A person whose credit history has been wrongfully disclosed or obtained, like a person whose driver’s-license information has been wrongfully disclosed or obtained, will often have no reason to know that her rights have been violated until she suffers some harm. But the Supreme Court nevertheless refused to apply the discovery rule, finding that the language of the FCRA demonstrated Congress’s intent to apply the occurrence rule and that “[t]he FCRA does not govern an area of the law that cries out for application of a discovery rule” *Id.* at 28. If a claim under the FCRA that a plaintiff’s credit information was improperly disclosed or obtained does not “cr[y] out for application of a discovery rule,” then neither does a claim under the DPPA that a plaintiff’s driver’s-license information was improperly disclosed or obtained.

Second, courts have often pointed out that Congress enacted the DPPA “in response to safety concerns about the ease with which individuals could obtain this information from the state, as well as concerns about direct marketers who used this information for commercial purposes without drivers’ consent.” *Cook v. ACS State & Local Solutions, Inc.*, 663 F.3d 989, 992 (8th Cir. 2011). Thus, as other judges have noted, “the main injury targeted by the DPPA is harm that would readily be knowable in conjunction with, or soon after, the DPPA violation,

because someone uses the data in reaching out to the plaintiff for threatening or advertising purposes.” *Kost*, 2013 WL 6048921, at *8. In other words, application of the discovery rule is not justified because when a plaintiff suffers harm on account of a DPPA violation, that harm will generally occur soon after the DPPA violation, and the plaintiff will be aware of that harm.

It is true, as Potocnik argues, that the DPPA applies to more than just the use of personal information to harass or annoy. The DPPA prohibits obtaining or disclosing personal information even when the information is not put to any particular use, and even when the plaintiff suffers no real harm. (The DPPA authorizes the recovery of statutory damages.) But letting this kind of “harmless” violation drive the statute-of-limitations inquiry would be to let the tail wag the dog. Absent an improper use, no one will ever have reason to suspect that their DPPA rights have been violated. The practical effect of adopting the discovery rule, therefore, would be to abolish the statute of limitations in cases not involving an improper use. In other words, the statute of limitations would most often bar the claims of plaintiffs whose personal information was used to harm them (the most serious cases), and least often bar the claims of plaintiffs whose personal information was not used in any way (the least serious cases). It seems highly doubtful that Congress intended this result. Statutory damages are in the nature of a penalty, *see UnitedHealth Group Inc. v. Hiscox Dedicated Corp. Member Ltd.*, No. 09-0210 (PJS/SRN), 2010 WL 550991, at *8-9 (D. Minn. Feb. 9, 2010), and the Supreme Court has said that “it would be utterly repugnant to the genius of our laws if actions for penalties could be brought at any distance of time.” *Gabelli*, 133 S. Ct. at 1223 (citation and quotations omitted).

Undoubtedly, application of the occurrence rule will cause some people to lose valid claims about which they had no reason to be aware. But application of the discovery rule would

indefinitely extend the limitations period for plaintiffs who suffer no actual damages while doing little or nothing to help plaintiffs who suffer precisely the kind of harm that prompted passage of the DPPA. The Court believes it far more likely that Congress intended the former, rather than the latter, of these two imperfect scenarios. *See Rotella v. Wood*, 528 U.S. 549, 544 (2000) (rejecting a discovery rule that “might have extended the limitations period to many decades, and so beyond any limit that Congress could have contemplated” because “[p]reserving a right of action for such a vast stretch of time would have thwarted the basic objective of repose underlying the very notion of a limitations period”).

The Court therefore holds that the occurrence rule applies and that any DPPA claims based on acts that occurred more than four years before Potocnik filed this action are time-barred. Carlson’s motion for judgment on the pleadings is granted as to those claims.

C. Section 1983

Potocnik brings three types of claims under § 1983 against the Commissioners and Carlson: a DPPA claim, a Fourth Amendment claim, and a Fourteenth Amendment invasion-of-privacy claim.

1. DPPA

Potocnik seeks to pursue her DPPA claims both directly (as discussed above) and through the vehicle of a § 1983 action. The Court concludes, however, that Potocnik cannot use § 1983 to sue for violation of her rights under the DPPA.⁶

⁶The Court notes that any § 1983 DPPA claim against the Commissioners would fail on the merits anyway, as the Court has already concluded that Potocnik failed to state a DPPA claim against them.

Section 1983 “authorizes suits to enforce individual rights under federal statutes as well as the Constitution.” *City of Rancho Palos Verdes v. Abrams*, 544 U.S. 113, 119 (2005). To successfully pursue a § 1983 claim based on the violation of a federal statute, the plaintiff must first show that the statute “creates an individually enforceable right in the class of beneficiaries to which he belongs.” *Id.* at 120. If the statute creates such a right, then there is a rebuttable presumption that the plaintiff may bring a § 1983 claim to recover for a violation of the statute. *Id.* But the defendant may rebut the presumption by showing that Congress did not intend for the federal right to be vindicated through a § 1983 action. *Id.* “[E]vidence of such congressional intent may be found directly in the statute creating the right, or inferred from the statute’s creation of a ‘comprehensive enforcement scheme that is incompatible with individual enforcement under § 1983.’” *Id.* (quoting *Blessing v. Freestone*, 520 U.S. 329, 341 (1997)).

Section 1983 is most often used to enforce federal rights for which there is otherwise no judicial remedy. *See id.* at 121 (“in *all* of the cases in which we have held that § 1983 *is* available for violation of a federal statute, we have emphasized that the statute at issue . . . *did not* provide a private judicial remedy”). “The provision of an express, private means of redress in the statute itself is ordinarily an indication that Congress did not intend to leave open a more expansive remedy under § 1983.” *Id.* In particular, where the remedy established in the statute is limited in ways that § 1983 is not, the § 1983 remedy is not available. *Id.*

Applying these principles, the Court concludes that § 1983 is not available as a means to enforce the DPPA. The Court does not doubt that the DPPA creates individually enforceable rights or that Potocnik belongs to the class of individuals that the statute is meant to protect. But

the DPPA includes its own more-restrictive private right of action, which, as the Supreme Court has said, means that Congress did not intend to permit § 1983 actions to enforce the statute.

The private remedy available under the DPPA is more restrictive than the remedy available under § 1983 in at least two ways. First, § 1983 claims have a different (and, in Minnesota, longer) statute of limitations. *Anunka v. City of Burnsville*, 534 Fed. Appx. 575, 576 (8th Cir. 2013) (per curiam) (in Minnesota, § 1983 claims are subject to a six-year statute of limitations). Allowing a plaintiff to assert DPPA rights via § 1983 would effectively abrogate the four-year statute of limitations that applies to DPPA claims. Most likely, that is exactly why Potocnik pleaded DPPA claims under both the DPPA and § 1983 — to gain the benefit of the longer statute of limitations that would apply to DPPA claims under § 1983.

Second, as noted earlier, the DPPA precludes lawsuits against states and state agencies, no matter what relief is sought by the plaintiff. *See* 18 U.S.C. § 2724(a) (creating a cause of action against a “person” who unlawfully obtains, discloses, or uses personal information from a motor-vehicle record); 18 U.S.C. § 2725(2) (excluding states and state agencies from the definition of “person”). Under § 1983, however, a plaintiff can sue state officials in their official capacities for injunctive relief. *See Murphy v. Arkansas*, 127 F.3d 750, 754 (8th Cir. 1997); *see also Will*, 491 U.S. at 71 (suit against state official in his official capacity is a suit against the state itself). Hence, permitting a plaintiff to assert DPPA rights in a § 1983 action would allow the plaintiff to circumvent the limits on relief available in direct actions under the DPPA.

Potocnik points out that the only federal appellate court to have addressed the issue held that a plaintiff may enforce DPPA rights through § 1983. *See Collier v. Dickinson*, 477 F.3d 1306, 1310-11 (11th Cir. 2007). The Court does not find *Collier* persuasive, however. *Collier*

did not apply or even cite *City of Ranchos Palos Verdes*, which made clear that the existence of a more-restrictive private remedy is the “dividing line” between federal rights that are enforceable under § 1983 and those that are not. *City of Rancho Palos Verdes*, 544 U.S. at 121. Because the private remedy available under the DPPA is more restrictive than the remedy available under § 1983, the Court concludes that the DPPA may not be enforced through § 1983. The Court therefore grants defendants’ motions as to these claims.

2. Fourth Amendment

Potocnik alleges that the Commissioners and Carlson violated her rights under the Fourth Amendment. To state a claim under the Fourth Amendment, however, Potocnik must show that she was subjected to an unreasonable search or seizure. *See* U.S. Const. amend. IV (prohibiting “unreasonable searches and seizures”). No court has ever held that accessing a driver’s-license database constitutes a search or seizure within the meaning of the Fourth Amendment. Potocnik thus fails to state a claim under the Fourth Amendment. Moreover, even if there were some theory under which defendants might be considered to have conducted a search or seizure, they would be entitled to qualified immunity.⁷ *See Bishop v. Glazier*, 723 F.3d 957, 961 (8th Cir. 2013) (“In § 1983 actions, qualified immunity shields government officials from liability unless their conduct violated a clearly established constitutional or statutory right of which a reasonable official would have known.”).

⁷Although Carlson pleaded the defense of qualified immunity, he chose not to raise that defense in his motion for judgment on the pleadings. ECF No. 27 at 10 n.4.

3. Fourteenth Amendment

Potocnik alleges that defendants violated her right to privacy under the Fourteenth Amendment by disclosing or obtaining private information about her. It is difficult to tell, however, exactly what private information Potocnik alleges was disclosed or obtained. Potocnik generally alleges that the DVS database contains “Private Data,” which she generally defines to include name, date of birth, driver’s-license number, address, driver’s-license photo, height, weight, social-security number, health and disability information, and eye color. Compl. ¶ 100. Potocnik then alleges that law-enforcement officers (including Carlson) obtained her “Private Data,” and that the Commissioners created and maintained a database containing her “Private Data.” Compl. ¶¶ 112, 117-18. But Potocnik also includes in her complaint an itemized list of the specific information that she alleges was obtained or disclosed about her, and that list conspicuously fails to include her social-security number or any health or disability information. Compl. ¶ 116.

Having carefully considered the allegations in Potocnik’s complaint, the Court concludes that Potocnik has not plausibly alleged that defendants disclosed or obtained any health or disability information about her. The Court does, however, believe that Potocnik has sufficiently alleged that defendants disclosed or obtained her social-security number, although it is a close question given that Potocnik inexplicably left that item off of her itemized list. The difference is that, while almost everyone who applies for a driver’s license will disclose a social-security number, only a subset of applicants will need to disclose any health or disability information. Potocnik does not allege that she provided any health or disability information to DPS in order to obtain a driver’s license, nor does she allege that she has any health condition or disability that

would need to be disclosed. For that reason, any allegation that defendants disclosed or obtained such information about Potocnik from the DVS database is conclusory and not plausible.

In addition, the Court notes that Potocnik's allegations regarding Carlson's harassing phone calls indicate that Carlson must have obtained information about Potocnik from sources other than her DVS record. For example, Potocnik alleges that Carlson knew whom she was dating, knew where she worked and went to school, and knew that she planned to take the Peace Officers Standards and Training Test — all information that would not have come from her DVS record. In her brief, however, Potocnik focuses only on the information gained from her DVS record. ECF No. 29 at 16-22. For purposes of Potocnik's constitutional-right-to-privacy claim, therefore, the Court will assume that defendants disclosed or obtained Potocnik's home address, photograph, date of birth, eye color, height, weight, driver's-license number, driving record, and social-security number.

With that clarification, it is apparent that Potocnik has not pleaded a viable claim for invasion of her constitutional right to privacy. The Eighth Circuit has set a demanding standard for such claims: “[T]o violate [a person's] constitutional right of privacy the information disclosed must be either a shocking degradation or an egregious humiliation of her to further some specific state interest, or a flagrant bre[a]ch of a pledge of confidentiality which was instrumental in obtaining the personal information.” *Eagle v. Morgan*, 88 F.3d 620, 625 (8th Cir. 1996) (quoting *Alexander v. Peffer*, 993 F.2d 1348, 1350 (8th Cir. 1993)).

Applying this strict standard, the Eighth Circuit has refused to recognize a constitutional right of privacy in precisely the type of information that Potocnik alleges is contained in her DVS record. *See Spurlock v. Ashley Cnty.*, 281 Fed. Appx. 628, 629 (8th Cir. 2008) (no violation of

privacy where sheriff's office disclosed intake sheet containing social-security number to third parties, who then distributed the information to others);⁸ *McCaslin v. Campbell*, 108 F.3d 1382, 1997 WL 148824, at *1-2 (8th Cir. Apr. 2, 1997) (affirming dismissal of privacy claims alleging release of social-security numbers and other information because, to the extent the information was not already public, it “did not involve the most intimate aspects of human affairs”); *Eagle*, 88 F.3d at 627-28 (rejecting privacy claim based on allegedly improper searches of computerized criminal records containing “identifiable descriptions” and other information).

Potocnik nevertheless argues that defendants violated her constitutional right to privacy because they breached a promise, embodied in state law, that her DVS record would be kept confidential. It is true that the Eighth Circuit has remarked in dicta that a “flagrant bre[a]ch” of a promise of confidentiality that was “instrumental” in obtaining personal information may state a claim for a violation of the constitutional right to privacy. *Alexander*, 993 F.2d at 1350. So far as the Court can discover, however, the Eighth Circuit has never actually found such a violation — or, for that matter, even addressed a claim of such a violation. Thus, the Eighth Circuit has never explained the difference between a “flagrant” breach and a “non-flagrant” breach.

The Eighth Circuit took the “flagrant breach” language from *Davis v. Bucher*, 853 F.2d 718 (9th Cir. 1988), in which a prison guard found nude photographs of an inmate's wife among the inmate's possessions and exhibited them to two other inmates. *Id.* at 719. The guard also later made disparaging comments about the wife's anatomy that were overheard by at least one guard and one inmate. *Id.* Despite these egregious facts, the Ninth Circuit affirmed the grant of

⁸The facts in *Spurlock* are recited in the district-court opinion. See *Spurlock v. Ashley Cnty.*, No. 05-1048, 2007 WL 858624, at *1 (W.D. Ark. Mar. 20, 2007).

summary judgment against the inmate on his constitutional-right-to-privacy claim, explaining that “the injury alleged by Davis is not one of constitutional magnitude.” *Id.* at 720. In the course of its analysis, the Ninth Circuit distinguished *Fadjo v. Coon*, 633 F.2d 1172 (5th Cir. 1981), in which, according to the Ninth Circuit, “the state’s investigator flagrantly breached a pledge of confidentiality, which had been instrumental in obtaining the personal information.” *Id.* at 721.

In *Fadjo*, a state official was assigned to investigate a suspicious disappearance. *Fadjo*, 633 F.2d at 1174. During the investigation, the official obtained unspecified information from Fadjo, who was the named beneficiary of six insurance policies on the life of the person who had disappeared. *Id.* According to Fadjo, the information involved “the most private details of his life.” *Id.* The official promised Fadjo that the information was absolutely privileged under Florida law and would never be revealed to anyone. *Id.* In breach of this promise, the official disclosed the information, which eventually made its way to the insurance companies. *Id.* As a result of the breach, Fadjo alleged, he was forced to move out of the county and was unable to obtain meaningful employment. *Id.*

The Fifth Circuit found that these allegations sufficiently stated a claim for violation of the constitutional right to privacy. *Id.* at 1175-77. Although the Fifth Circuit did not describe the type of information that was disclosed, the court made it clear that the information was “intimate.” *Id.* at 1176 (“We note first that Fadjo’s case is distinguishable from Paul since it involves the revelation of intimate information obtained under a pledge of confidentiality rather than the dissemination of official information.”). The Fifth Circuit later distinguished *Fadjo* on this basis, holding that the release of non-private information that the defendant had promised not

to disclose did not give rise to a constitutional claim. *Cinel v. Connick*, 15 F.3d 1338, 1342 (5th Cir. 1994).

Given the Eighth Circuit's reluctance to expand the constitutional right of privacy and the extremely high standards that it sets for such claims, the Eighth Circuit would probably have not found a viable constitutional claim under the facts alleged in *Fadjo*. *Cf. Riley v. St. Louis Cnty.*, 153 F.3d 627, 631 (8th Cir. 1998) (police officers who photographed plaintiff's deceased son in his casket, displayed photograph at public forum, and publicly blamed his death on his gang activities did not violate constitutional right to privacy). But even if the Eighth Circuit would follow *Fadjo*, *Fadjo* is distinguishable from this case because it involved the disclosure of "intimate" information that the plaintiff described as "the most private details of his life." *Fadjo*, 633 F.2d at 1174, 1176.

The information about Potocnik in the DVS database is statutorily defined as private, but it cannot fairly be said to include the "most private details" of her life. Moreover, unlike the plaintiff in *Fadjo*, Potocnik was not promised that her information would never be revealed to anyone; to the contrary, there are many scenarios under which Potocnik's DVS driver's-license information could have been lawfully obtained by others, including the defendants in this case. For that reason, the Court does not believe that Potocnik has pleaded the type of "flagrant" breach of a promise of confidentiality that the Eighth Circuit referred to in *Alexander*. The Commissioners created and currently maintain a database containing DVS records to which law-enforcement officers and others are granted password-protected access. The fact that access to the database is sometimes abused does not render the Commissioners' creation and maintenance of the database "flagrant." And Carlson, of course, never made any promise to Potocnik about

the confidentiality of her information, and thus did not “flagrantly” violate such a promise. Moreover, the only arguably private information that Carlson obtained was Potocnik’s social-security number, and Potocnik does not allege that Carlson used that information in any way or disclosed it to anyone else. The Court therefore concludes that Potocnik has failed to state a claim for a violation of her constitutional right to privacy.

Finally, even if Potocnik could state a constitutional claim, defendants would be entitled to qualified immunity.⁹ Potocnik does not have a clearly established constitutional right of privacy in the information contained in her DVS record, nor is it clearly established that the Commissioners could be held liable merely for making that information available to law-enforcement officers who might misuse it. The Court therefore grants the defendants’ motions as to Potocnik’s claim for violation of her constitutional right to privacy.

D. Intrusion Upon Seclusion

Finally, Potocnik brings a state-law claim of intrusion upon seclusion, which is a form of invasion of privacy. The elements of an intrusion-upon-seclusion claim are (1) an intrusion (2) into some matter in which a person has a legitimate expectation of privacy (3) that would be highly offensive to the ordinary reasonable person. *Swarthout v. Mut. Serv. Life Ins. Co.*, 632 N.W.2d 741, 744-45 (Minn. Ct. App. 2001). The conduct must be of a nature to which a reasonable person would strongly object. *Id.* at 745.

Although Potocnik alleges that Carlson made highly intrusive and harassing phone calls, those phone calls do not form the basis of her intrusion-upon-seclusion claim. Instead, the sole basis of her claim is that defendants intruded upon her seclusion “[b]y improperly obtaining

⁹Again, Carlson did not move for judgment on the basis of qualified immunity.

Potocnik’s private personal information for impermissible reasons” Compl. ¶ 301. Unlike her constitutional claim, however, Potocnik’s claim against Carlson is based on more than just the information in her DVS record: In her brief, she mentions that Carlson obtained her “driver’s license information *and other private information*” ECF No. 29 at 25-26 (emphasis added).

To the extent that Potocnik’s state-law claim is based on the information in the DVS database, it fails as a matter of law. The Eighth Circuit has held that obtaining a social-security number is not a tortious intrusion upon seclusion. *Phillips v. Grendahl*, 312 F.3d 357, 373 (8th Cir. 2002) (“Discovery of that [social-security] number therefore does not fit the profile of intrusion upon seclusion.”), *abrogated on other grounds*, *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47 (2007). And as for the remaining information in the DVS database, the Court agrees with other courts in this district that the act of obtaining or disclosing such information would not be highly offensive to an ordinary reasonable person.¹⁰ See *Nelson v. Jesson*, No. 13-340 (RHK/JJK), 2013 WL 5888235, at *8 (D. Minn. Nov. 1, 2013) (noting that much of the information is publicly available and that most people readily produce their driver’s licenses to confirm their age or identity).

To the extent that Potocnik’s claim is based on the non-DVS information that Carlson allegedly obtained, the Court also finds that the claim fails as a matter of law. In her brief, Potocnik barely mentions the non-DVS information and does not specifically describe any of it, leaving the Court to guess which items of information are the basis of her claim. The Court assumes, however, that Potocnik is referring to Carlson’s knowledge of whom she was dating;

¹⁰As noted, Potocnik has not adequately alleged that there is any health or disability information in her DVS record.

where she worked and attended school; her plan to take the Peace Officers Standards and Training Test; and the facts surrounding her sister's murder. Again, although Carlson's *use* of this information to harass and berate Potocnik would likely be highly offensive to an ordinary reasonable person, Potocnik's claim is based solely on the ground that Carlson improperly *obtained* it. Compl. ¶ 301.

Potocnik does not, however, allege any facts showing that Carlson improperly obtained the non-DVS information. Even if she had, Potocnik cites no authority for the proposition that improperly obtaining information constitutes intrusion upon seclusion regardless of the nature of the information obtained. To the contrary, the tort requires both that there be a highly offensive intrusion and that it be into some matter in which a person has a legitimate expectation of privacy. *See Phillips*, 312 F.3d at 372-73 ("The use of improper methods to obtain information, such as a request that violates the Fair Credit Reporting Act, does not necessarily make the acquisition of information highly offensive, if the information could just as well have been obtained by proper means.").

Potocnik does not have a legitimate expectation of privacy in the non-DVS information such that its discovery, without more, would be highly offensive to the ordinary reasonable person. As Potocnik alleges, her sister's murder was widely reported in the news media, Compl. ¶ 56, and information about whom she is dating and where she works is not the kind of information that is "a very private part of one's person" and "generally known to others only by choice." *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 235 (Minn. 1998) (recognizing the tort of intrusion upon seclusion in a case involving the unauthorized distribution of a nude photograph); *see also Phillips*, 312 F.3d at 365-66, 372-73 (holding that a credit report that

mentioned a child-support order and contained a social-security number, addresses of former employers, and a list of credit accounts was insufficient to support a claim of intrusion upon seclusion). The Court therefore grants defendants' motion as to Potocnik's claim of intrusion upon seclusion.

ORDER

Based on the foregoing, and on all of the files, records, and proceedings herein, IT IS HEREBY ORDERED THAT:

1. Defendants Michael Campion and Ramona Dohman's motion to dismiss [ECF No. 7] is GRANTED.
2. All claims against defendants Michael Campion, Ramona Dohman, and the unnamed DPS defendants are DISMISSED WITH PREJUDICE AND ON THE MERITS.
3. Defendant Walter Carlson's motion for partial judgment on the pleadings [ECF No. 25] is GRANTED.
4. With the exception of claims under the Driver's Privacy Protection Act that are based on acts that occurred on or after August 1, 2009, all claims against defendant Walter Carlson are DISMISSED WITH PREJUDICE AND ON THE MERITS.

Dated: March 24, 2014

s/Patrick J. Schiltz
Patrick J. Schiltz
United States District Judge